



FOLEY & LARDNER LLP

Quon v. Arch Wireless—A Lesson Regarding Employee Monitoring

**Andrew B. Serwin
402 W. Broadway
Suite 2100
San Diego, CA 92101
aserwin@foley.com**

A History of Wiretapping

- Warrantless wiretapping has a long history.
 - The Church Commission report.
- Initially wiretapping was not held to violate any privacy rights.

A History of Wiretapping

- *Katz* was one of the first cases to recognize a privacy right in wire communications.
- Title III of the Omnibus Crime Control and Safe Streets Act resulted.
- This ultimately became the ECPA.

Other Federal Privacy Theories

- The Fourth Amendment.
 - This is not seen as a general privacy protection, but there are specific restrictions, including the warrant requirement that are based upon the Fourth Amendment.
- There are Fourth Amendment implications when the government seeks to obtain evidence of a crime.

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.*)

- There are two portions of the ECPA
 - The Wiretap Act; and
 - The Stored Communications Act
- This is a temporal distinction
- There are also certain additional restrictions on public providers.

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.*)

- Wiretap Act and Councilman.
 - Prohibits “interception” of “electronic communications”.
 - "electronic communication" "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photooptical system that affects interstate or foreign commerce,"
 - Does not include electronic storage as does the definition of “wire communications” or the storage definition of the Stored Communications Act.

Electronic Communications Privacy Act

18 U.S.C. § 2510 *et seq.*

- What is storage?
 - Is it on a hard drive?
 - Is it in memory—RAM?
 - Is it in memory on the wire?
- The lower court opinion in *Quon* was notable on this issue.

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.*)

- Applies mostly for businesses in the employee context.
- Two potential exceptions:
 - protect the provider, another provider, or a user, from fraudulent, unlawful or abusive use of such service; or
 - a person employed or authorized, or whose facilities are used, to forward such communication to its destination

General Employee Concerns

- Other issues to consider when you are drafting your policy.
 - Does the absence of a policy create a reasonable expectation of privacy?
 - What role does password protection play?
 - What role to physical characteristics of an office play?
 - Is ownership of equipment determinative?

Employees and the Attorney-Client Privilege

- Even with a monitoring policy, there can be other concerns about reviewing communications with an employee's attorney, even if done on a work computer, though the cases are mixed.

Quon v. Arch Wireless

- The case involves 4 plaintiffs—two members of a SWAT team, a dispatcher and Jeff Quon's wife.
- The role of the policy in the case is important to note.

Quon v. Arch Wireless

- Technology at issue was a text message capable pager that was supported by a third-party.
- Both Quon and Trujillo had the same pager.

Quon v. Arch Wireless

- What issues were presented in the case:
 - Was Arch an ECS v. a RCS?
 - What protections do employees have in text messaging?
 - What role does an employee monitoring policy play in setting the employee's expectation of privacy?
 - What role does “operational reality” play?
 - What impact do public records laws have?

Quon v. Arch Wireless

- ECS v. RCS.
 - This issue was relevant because under 2702 a “subscriber” cannot get content without consent of a recipient.
- Employee policies.
 - A general employee policy was in place, but was not consistently applied in the case.
- Operational reality.
 - Here the Department had varied its announced policy by conduct.
- The role of personal use.
- Public records laws.

Quon v. Arch Wireless

- What are the takeaways:
 - Review your policy, particularly if it is “general”;
 - Courts will look behind your policy;
 - Ownership is not determinative;
 - Public records laws may not be determinative.

What About State Law?

- *Quon* did not address California law as the issue was waived on appeal.
- In other cases, California's Wiretap law has been applied to certain forms of communications.

State Wiretap Laws

- Most states have a wiretap law that covers electronic communications as well.

State Electronic Monitoring Laws

- Two party consent states present unique issues.
- These states include:
 - California;
 - Connecticut;
 - Delaware;
 - Florida;
 - Illinois;
 - Maryland;
 - Massachusetts;
 - Nevada;
 - New Hampshire;
 - Pennsylvania;
 - Vermont; and
 - Washington.

California's Invasion of Privacy Act

- Cal. Penal Code § 631.
 - Prohibits 3 distinct acts:
 - Intentional wiretapping;
 - Willful attempts to learn the contents of a communication in transit; and
 - Attempts to publicize information obtained in either of the above ways.
 - Litigation privilege may apply and provide some immunity.

California's Invasion of Privacy Act

- Application of California law to calls originating out of state.
 - *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal.4th 95 (2006).

State Employee Email Monitoring Laws

- Connecticut
 - Requires notice and posting of notice of the employer's monitoring policies
- Delaware
 - Requires that notice be given every day to the employee
- Certain exceptions apply for investigations
- Civil penalties are available
- *Fischer v. Mt. Olive Lutheran Church*

The Computer Fraud and Abuse Act (CFAA)

- Applies in several situations.
 - To a person's use or access of a “protected computer” if done with intent—
 - If it exceeds the scope of authorization; or
 - Is done to further a fraud—which means damage to property via dishonesty, schemes or other artifices.
 - Transmission of code.
 - If there is access and damage.

The Computer Fraud and Abuse Act (CFAA)

- There are certain prerequisites to a claim:
 - Aggregated damage of over \$5,000;
 - Potential modification or impairment of a medical diagnosis, examination, treatment or care of a person;
 - Physical injury;
 - A threat to public health or safety; or
 - Damage to a government computer that is used for certain purposes.

The Computer Fraud and Abuse Act (CFAA)

- Common situations.
 - Employers with trade secrets.
 - Hackers.
 - Dissemination of malware or viruses.
- Subpoenas.
 - *Theofel v. Farey – Jones*, 359 F.3d 1066 (2004).

State Computer Crime Laws

- Most states have these laws and they generally track federal law, though many are broader.
- Most do not require an “interruption in service.”

California's Computer Crime Law

- Cal. Penal Code § 502.
 - Knowing access to a computer without permission to commit certain acts, including to defraud is a crime.
 - Knowing access to a computer without permission to copy data is also a crime.
 - Improper use of computer services, as well as introducing computer contaminants also violates this law.
 - Many other acts, including improper access to software, are covered as well.

California's Computer Crime Law

- Civil remedies exist under California's law, as do criminal penalties.

State Computer Crime Laws

- Alabama
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Iowa
- Kansas
- Louisiana
- Maine
- Maryland
- Massachusetts
- Minnesota
- Mississippi
- Missouri
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- Texas
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

State Public Utility Restrictions on Telephone Records

- California Public Utilities Code Section 2891
- California Code of Civil Procedure Section 1985.3

California Common Law and Pretexting

- *Taus v. Loftus*, 40 Cal.4th 683 (2007),
*Information Security and Privacy: A
Practical Guide to Federal, State and
International Law*, § 25:11.